(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/009473 A1

(51) International Patent Classification[7]: B65D 90/22

(21) International Application Number: PCT/IB2003/002860

(22) International Filing Date: 18 July 2003 (18.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002/5797 19 July 2002 (19.07.2002) ZA

(71) Applicant and
(72) Inventor: GREYLING, Jan, Christoffel [ZA/ZA]; 14 Diana Circle, The Reeds, 0158 Centurion (ZA).

(74) Agent: MACKENZIE, Colin; Adams & Adams, Adams & Adams Place, 1140 Prospect Street, Hatfield, P O Box 1014, 0001 Pretoria (ZA).

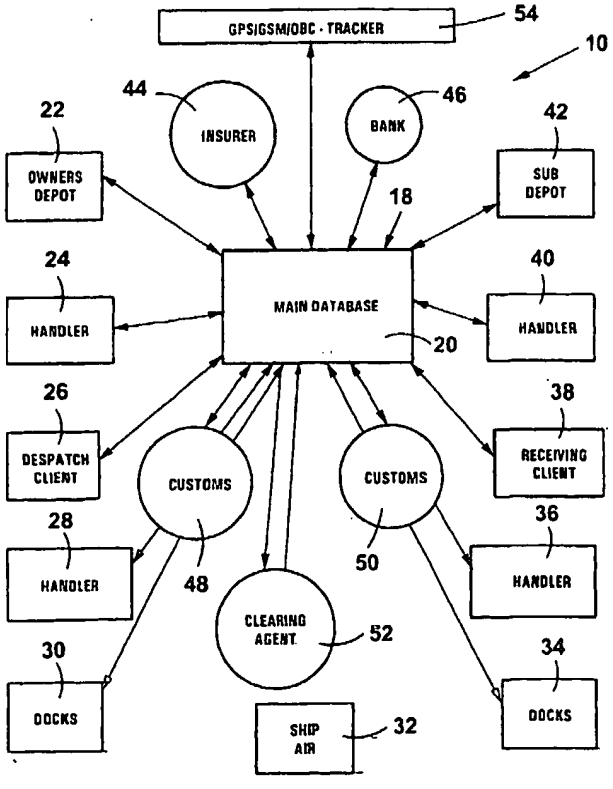
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: CONTAINER MANAGEMENT SYSTEM



(57) Abstract: The invention provides a container having a slave unit mounted therein for controlling the operation of lock of the container and for monitoring the status of the container. An interface is provided whereby the slave unit can communicate with a remote controller. The invention further provides a container management system for managing the transportation of the containers.

WO 2004/009473 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTAINER MANAGEMENT SYSTEM

THIS INVENTION relates to a container. In addition it relates to a container management system. It also relates to a method of controlling access to a container. Further, it relates to a method of managing the transportation of goods from a supplier to a receiver. The invention further relates to a slave unit.

Containers for the transportation and handling of goods are well known. The containers may be transported by road, sea and/or air. Theft of the contents of the containers occurs frequently and thieves may obtain an indication of the contents of the container from the standard documentation which accompanies the container. Further, although conventional containers are locked from the outside and thereafter sealed, sophisticated thieves typically gain unauthorized access to the container, remove the contents, and then re-seal the container making it extremely difficult to ascertain when the goods may have been stolen, for example, to determine liability.

According to one aspect of the invention there is provided a container which includes

a body defining a goods receiving cavity within which goods are receivable, the body having an access opening through which goods can be introduced into and removed from the cavity;

a closure element for closing the access opening;

a lock for locking the closure element releasably in a closed position; and

a lock actuator for displacing the lock between a locked position and an unlocked position, the lock actuator being positioned inside the

container body and having an interface for communicating with a remote controller positioned outside the container.

The container may include a container slave unit at least part of which is mounted within the body for monitoring data relating to the container, the lock actuator forming part of the slave unit. The slave unit may be mounted at the time of the manufacture of the container. Instead it may be retrofitted to an existing container.

The slave unit may include a power source and at least part of the slave unit may be dismountably mounted in the container. The power source may be in the form of a rechareable battery. In this regard, the battery may be rechargeable from an electrical mains supply. Instead, the battery may be rechargeable via a battery charger arrangement. The battery charger arrangement may include a solar panel and/or a wind powered electrical generator. The fact that the slave unit is dismountably mounted in the container permits its removal and mounting in a different container.

The slave unit may include a transmitter and a receiver for communicating in a wireless fashion with a remote controller having a complementary transmitter and receiver.

The slave unit may include an antenna to permit communication with a remote controller by radio wave.

The antenna is typically positioned within the container body, and where appropriate, contained in a casing which serves to protect the antenna and resist tampering therewith.

The slave unit may include a unique identifier, uniquely to identify the container within which it is mounted.

In the context of this aspect of the invention, the term "container" is to be construed broadly to include any lockable enclosure including bulk transportation containers, closed body vehicles, safes, strongboxes and the like.

When the container is of a construction which inhibits the transmission of radio signals between the inside and the outside the container, then the container may include a transmission opening adjacent to which the antenna is positioned. In the case of bulk transportation containers, the antenna may be positioned in proximity to a door hinge which the Inventor has found permits the transmission of radio waves.

The radio wave communication may include GPS (Global Positioning System) and/or a communication network eg GMS (Global System for Mobile Communications).

The container may include tamper detection means for monitoring tampering with the container.

The tamper detection means may include a light sensor for sensing light within the container.

The tamper detection means may include a movement sensor sensing unauthorised movement of the container.

The container may include an alarm responsive to the tamper detection means for generating an audible alarm.

The container may include repelling means for repelling an unauthorised entry into the container.

The repelling means may include an atmospheric induction unit for releasing a chemical substance in the container.

The container may include a tracking device for tracking the geographical position of the container.

According to another aspect of the invention there is provided a container management system for managing transportation of containers, the system including

at least one container;

a container slave unit mounted to the container for monitoring data relating to the container;

a plurality of remote units provided at selected remote locations to which the container is to be transported, each remote unit being operable to communicate with the container slave unit to retrieve data from the slave unit; and

a control centre including a master database for storing management data relating to the container, the control centre being connected to connectable in communication with each remote unit to receive the data from the container slave unit and thereby update the management data.

The container slave unit may also monitor transportation data and function to control access to the container.

The method may include controlling access to the container by verifying the transportation data to determine if access to the container should be permitted and, if so, communicating an access code to the remote unit for communication to the slave unit thereby selectively to allow access to the container.

The control centre may include comparator means for comparing data sourced from each remote unit with data stored on the master database for generating a warning signal or alarm condition if the comparison indicates an excessive deviation from the data on the master database.

The management or base line data preferably includes a proposed or predefined transportation route which the container must follow. Accordingly, the control centre may monitor progress of the container along the route by receiving the transportation data from each remote unit at a remote location to which the container is to be transported. Typically, the remote locations include an owner of a container, a depot supplying the container, a handler or transportation company transporting the container to the supplier of goods, harbours, customs, dockyard, transit storage company, clearing agents, insurance companies, financial institutions, the receiver of the goods, or the like.

The management data in the master database may allow selective access thereto by the various remote units. For example, data on the contents or goods loaded in the container is typically only available to the

supplier and not to remote units at any intermediary remote locations. However, data on the progression of the container from the supplier to the receiver may be accessed from each remote unit along the way.

The control centre typically includes a personal computer (PC) or the like and the communications means may include a modem at the control centre which communicates via a telecommunications network to modems provided at each remote location. It is however to be appreciated that communication between the control centre and the remote units may be done by any wireless and/or hardwired communication network or link. In some embodiments of the invention, the communication means may be the Internet. Accordingly, each remote unit may communicate with a web site provided by the control centre thereby selectively to access the master database.

The slave unit may include an electrically operable locking arrangement for controlling access to the container. In a preferred embodiment, the locking arrangement is mounted within the container thereby to inhibit tampering, e.g. destruction, of the locking arrangement to obtain access to the container. Accordingly, authorization to open and/or close the container may be electronically controlled by appropriate data sourced from the control centre and communicated between the remote unit and the slave unit.

Communication between the slave unit and each remote unit is typically done in a wireless fashion. For example, the slave unit may include a transponder or the like and, accordingly, the remote unit may include a transponder interrogator connected to the PC. It is to be appreciated that, in addition or instead, the remote unit may include an

active transceiver for communication. Although in one embodiment a wireless portable data carrier is used to communicate with the slave unit, it is to be appreciated that a hardwired link can be used in addition or instead.

In another embodiment of the invention communication between the slave unit and the remote unit may be by radio wave, the slave unit then including an antenna which is typically positioned within the container. In order to resist tampering with the antenna when the container is open the antenna may be encapsulated in a protective material which does not interfere with radio transmission. When the container is of a construction which resists the transmission of radio waves then the antenna will typically be positioned adjacent to an opening in the container through which radio waves can pass. In the case of a bulk transportation container the opening may be provided by a door hinge.

The slave unit mounted within the container may include tamper detection means for monitoring tampering with the container. For example, the tamper detection means may include a light sensor for sensing light within the container e.g. by forced entry into the container, an aperture in the container, or the like. The detection means may include a movement sensor for sensing unauthorized movement of the container e.g. movement of the container when its access doors are open. Optionally, the slave unit may include an internal movement sensor, e.g. an ultrasonic movement sensor, infra-red movement sensor, or the like for sensing movement within the container. In addition, an impact sensor may be provided. In certain embodiments an audio/visual detection arrangement is provided.

Further, the slave unit may include an alarm responsive to the tamper detection means and/or the movement sensor for generating an audible alarm. In certain embodiments of the invention, the slave unit includes repelling means for repelling an unauthorized entrant into the container. The repelling means may be an atmospheric induction unit for releasing a chemical substance in the container e.g. intermittently over a period of time. An electrical or audio repelling means may also be provided.

The slave unit is typically microprocessor based including storage means for storing at least the transportation data for communication to the remote unit. Preferably, the slave unit includes a microcontroller e.g. a MCS 51 based controller or the like, which controls operation of the slave unit including its tamper detection means, movement sensor, communication means, locking arrangement, and the like. Accordingly, the microcontroller may be arranged to log or record (time and date stamp) a plurality of events relating to the container e.g. an attempt to gain unauthorized access to the container. When the container reaches its next remote location on route to the receiver, data from the storage means may be communicated to the remote unit on site and, thereafter, communicated to the control centre.

The slave unit typically includes its own power supply which is preferably rechargeable. The rechargeable power supply may be in the form of a battery. The battery may be rechargeable from an electrical mains supply. Instead, or in addition, a recharge arrangement such as a solar panel and/or a wind powered electrical generator may be provided. In a preferred embodiment, the slave unit includes a tracking device for

tracking the geographical position of the container or may interface with an existing tracking device.

In order to conserve power, the slave unit may include a sleep mode. The slave unit may enter the sleep mode when the container is stationary for an extended period of time, eg if the controller is parked whilst in transit. The slave unit may enter the sleep mode automatically after a predetermined period of time and/or in response to a signal sent to the slave unit. If, however, the tamper detection means and/or the movement sensor is activated then the slave unit is automatically returned to its active mode.

The system is typically used to manage the transportation of a plurality of containers. Accordingly, the slave unit typically includes a unique identifier, e.g. a unique identification code, uniquely to identify the container within which it is mounted. At least part of the slave unit may be dismountably mounted to the container. This permits the slave unit to be removed from one container and mounted in another container. The transportation data may include the identification code to identify the particular container with which it is associated. Upon communication of the transportation data to the control centre, its database may be updated to record status information as well as progress information on the container.

Accordingly, the invention extends to the transportation of goods from a supplier to a receiver in a container provided with a slave unit for monitoring data relating to the container which method includes

retrieving data from the slave unit at selected locations; and

comparing the retrieved data with data stored on a master database to check on the status of the container.

The method may include the prior step of entering the data in the master database at a control centre, comparing the retrieved data with the data on the master database including communicating the retrieved data from the or each selected location to the control centre, the method further including updating the data on the master database.

At least part of the slave unit may be mounted inside the container and data from the slave unit is retrieved in a wireless fashion.

The invention also extends to a container for transporting goods, the container including a slave unit as hereinbefore described.

The invention further extends to a slave unit for use in a container management system as described above.

Hence, according to another aspect of the invention there is provided a slave unit which is mountable in a lockable enclosure, the slave unit including

a controller for receiving data relating to a said lockable enclosure in which it is mounted; and

a communication interface for communication with a remote unit having a complementary communication interface.

The slave unit may include lock control means for controlling the operation of the lock of a lockable enclosure in which the slave unit is mounted.

The invention is now described, by way of example, with reference to the accompanying diagrammatic drawings.

In the drawings,

Figure 1 shows a schematic block diagram of a container management system in accordance with the invention;

Figure 2 shows a schematic block diagram of a slave unit, also in accordance with the invention, mounted in the container;

Figure 3 shows a schematic communication flow diagram of first time users of the system of Figure 1;

Figure 4 shows a schematic communication flow diagram of the system at a port of export;

Figure 5 shows a schematic communication flow diagram of the registration of role players in the container management system;

Figure 6 shows a schematic block diagram of a further embodiment of a container management system in accordance with the invention;

Figure 7 shows a schematic block diagram of alternative methods of communication between the slave units, remote units, and a control centre;

Figure 8 shows a schematic block diagram showing, in particular, the database arrangement of the control centre;

Figure 9 shows a schematic block diagram of a remote unit of the system of Figure 6 including an identification interface;

Figure 10 shows a schematic representation of the process of registering a container;

Figure 11 shows a schematic representation of the process when a client requests a container from a supplier;

Figure 12 shows a schematic representation of the process of assigning a container to a transaction or request;

Figure 13 shows a schematic representation of the process of transferring custodianship of a container;

Figure 14 shows a schematic representation of the process of unlocking/locking a container by a client;

Figure 15 shows a schematic representation of the process of bonding/unbonding and blocking/unblocking of containers by customs officials;

Figure 16 shows a schematic representation of the process invoived in uniocking a biocked or bonded container; and

Figure 17 shows a schematic representation of the process of registering a client/handler in the container management system.

Referring to the drawings, reference numeral 10 generally indicates a container management system, in accordance with the invention, for managing the transportation of a plurality of containers 12 (see Figures 3 to 5). The system 10 includes a container slave unit 14 (see Figure 2), a plurality of remote units in the form of personal computers (PCs) 16 which are provided at selected remote locations to which the container 12 is to be transported, and a control centre 18 which includes a main or master database (MDB) 20. As described in more detail below, the system 10 controls access to the container 12, and its progress from a predetermined point of departure, eg a supplier or exporter, to a predetermined destination is monitored.

Referring in particular to Figure 1 of the drawings, the system 10 includes a remote unit or PC 16 located at an owner's depot 22, a first handler 24, a despatch client or exporter 26, a second handler 28, export docks 30, means of transport 32 (air/ship), destination docks 34, a third handler 36, a receiving client or importer 38, a fourth handler 40, and a

sub-depot 42. Further, the system includes remote units or PCs 16 located at the premises of an insurer 44, a banker 46, export customs 48, import customs 50, and a clearing agent 52. A preferred feature included in the system 10 is a GPS, GSM, OBC or the like tracking system 54. The system 10 may include a tracking system making use of lower orbital satellites which do not have conventional GPS foot print communication restrictions.

The system 10 is arranged to manage and monitor the transportation process of a plurality of containers 12 from an initial request from the importer 38 or the exporter 26 as the case may be. Each container 12 is fitted with a slave unit 14 which is mounted in a secure casing within the container 12. The unit 14 includes a microprocessor based controller 56 e.g. an MCS 51 microcontroller unit or the like, alarm apparatus 58, an internal rechargeable battery 60, an impact sensor 62, a light sensor 64, a tilting sensor 66, repelling means in the form of an atmospheric induction unit 68, an actuator driven locking device 70, a tracking device 72 with its own internal battery 74 for communicating with the tracking system 54, a power point connection 76, and a communication interface 78 for communication with a portable data carrier, e.g. in the form of a Dallas memory button 79.

The controller 56 controls operation of the slave unit 14 and, in particular, is operable selectively to actuate the locking device 70 to enable access to the container 12. The slave unit 14 includes a unique identification code stored in storage means of memory of the controller 56 which uniquely identifies the container 12 to which the device 14 is mounted. In response to further unique codes sourced from the control centre 18 via the remote units or PCs 16 and via Dallas memory buttons

79, data is fed to the controller 56 which then controls access to the container 12 as described in more detail below. In a similar fashion, transportation data is communicated from the unit 14 to the control centre 18.

The controller 56 is connected to the light sensor 64, the tilting sensor 66, the alarm apparatus 58, and the atmospheric induction unit 68. The light and tilting sensors 64, 66 respectively are operable to trigger the alarm apparatus 58 when selected preconditions arise. In particular, the light sensor monitors when the light present within the container 12 exceeds a predetermined level, e.g. when the container 12 is broken into, whereupon the alarm apparatus 58 is activated. The controller 56 then time and date stamps the event which is then recorded for subsequent communication to the control centre 18. If the alarm condition is not rectified within a predetermined time period, the atmospheric induction unit 68 is then activated to create atmospheric conditions within the container intended to repel or discourage unauthorised access to the contents of the container 12, and the tracking device 72 is selectively activated.

The tilting sensor 66 is typically enabled by the controller 56 when several deliveries, each of part of the contents of the container 12, are made. For example, if selected items from the container 12 have been delivered to a specific location via a road transportation arrangement, and access doors of the container 12 are not properly closed and locked prior to vehicle movement i.e. the vehicle embarking on its next delivery, the tilting sensor 66 senses movement and activates the alarm apparatus 58 and the microcontroller 56 time and date stamps the event. The atmospheric induction unit 68 may then be activated as well. The impact sensor 62 is operable to sense manhandling of the container 12 which is

also time and date stamped by the controller 56. The power point connection 76 allows recharging of the battery 60 from an external mains power source. If desired, a battery charger (not shown) may be provided. The battery charger may include a solar panel and/or a wind powered electrical generator mounted to the container. Thus, the slave unit 14 monitors and records selected events relating to the container 12. The Dallas memory button 79 allows wireless communication of transportation data including data on the events between the slave unit 14 and the PC 16 provided at the specific remote location as described in more detail below.

Referring in particular to Figure 3 of the drawings, a first time buyer 80, e.g. an importer or local buyer 38, who purchases goods and requires them to be transported via the container 12 to his premises, may log-on and browse the Internet as shown at block 82, to gain access to the system web site 84. The web site 84 provides comprehensive details on the system 10 and includes links and information on service providers, container/vehicle owners, handlers, clearing agents, or the like who are participants in the system 10. The first time buyer 80 may then place an order with the supplier or exporter and request delivery via a service route (see Figure 1) as shown at block 86.

In a similar fashion, a first time supplier 88 who wishes to transport goods to a particular client, may also access and browse the Internet 82 and log-on the web site 84. The web site 84, as mentioned above, provides comprehensive details on service providers, container/vehicle owners, handlers, clearing agents, or the like. Thereafter, the first time supplier 88 may order an empty container 12 from a registered container owner at a depot 22 (see Figure 1) as shown at block 90 in Figure 3. Once the empty container is ordered, the container owner contacts the

control centre 18 to register the new supplier or exporter 26 as shown at block 92. The supplier's details are then loaded into the master database 20 (see block 94) and the supplier is then registered and linked to the master database 20. The container owner then contacts the handler 28 to deliver the empty container 12 to the exporter 26.

The first time buyer 80 and the first time supplier 88 are registered at the control centre 18 and comprehensive details are then fed into the master database 20. An owner depot 22 is then contacted to obtain a container 12 fitted with an associated slave unit 14. In particular, the owner depot 22 includes a PC 16 which is in communication with the control centre 18. Once a specific container 12 has been identified at the depot for use in transporting the goods to the receiver or importer 38, a Dallas memory button 79 is located proximate the communication interface 78 and unique identification details of the container 12 including the unit 14 are then communicated to the Dallas memory button 79. The button 79 is then taken to the PC 16 where the unique identification details are loaded into the PC 16 in a wireless fashion and communicated to the master database 20. The master database 20 then analyses the status of the container 12 which typically reflects an empty locked container whereupon the control centre 18 then communicates an "empty lock" and "unlock code" to the PC 16 at the owner's depot 22. The empty container can now be locked and unlocked via the Dallas memory button 79 which communicates an appropriate code to the unit 14 which, in turn, activates the locking device 70.

The specific container 12 for transporting the goods with its unique identification code and a proposed transportation route is then registered with the master database 20. The proposed transportation route identifies

various remote locations or handling points through which the container should pass on its way to the receiver or importer 38. At each remote location data is communicated between PCs 16 at the location and the slave unit 14 and the master database 20 is updated. Accordingly, the master database 20 maps or monitors progress of the container 12 during the transportation process. In certain embodiments, registration of the container 12 at the master database 20 is only accepted if the status received by the control centre 18 reflects an empty locked container 12 at the owner's depot 22. A unique "empty container unlock code" is then generated in the master database 20 and the code is only accessible by the despatch client or exporter 26.

Once the container 12 has been registered by the owner's depot 22 it is conveyed or transported to the despatch client or exporter 26 via the handler 24. The handler 24 also includes a PC 16 for communicating with the control centre 18. The container 12 is then transported to the despatch client 26 and the Dallas memory button 79 is then located against the communication interface 78 to retrieve unique identification data from the unit 14. Once the unique identification data has been retrieved it is communicated in a wireless fashion to a PC 16 located at the despatch client 26. The despatch client or exporter 26 then receives "empty lock" and "unlock codes" from the master database 20 thereby enabling them to open the container 12 so that the goods ordered may be packed therein. In particular, the "empty lock" and "unlock codes" are received by the PC 16, and are communicated to the Dallas memory button 79 which, in turn, is placed in proximity to the communication interface 78 to communicate the codes to the unit 14. The codes then allow the container 12 to be locked and unlocked as the case may be and the despatch client or exporter 26 enters data on the handler and importer

or receiving client 38 into the master database 20 via a PC located at the despatch client or exporter 26.

The exporter or despatch client 26 also enters cargo details which are loaded into the master database 20. The details on the cargo are not accessible by any of the other intermediaries or remote locations and, thus, the contents of the container 12 are kept secret for security purposes. Comprehensive details of the cargo are only accessible by the receiving client or importer 38 when a specific unique code is communicated to the control centre 18. Thus, access to data in the master database 20 is restricted and only selected information can be accessed by different intermediaries involved in the transportation of the container 12.

As mentioned above, once the container 12 has been loaded, an appropriate command is given via the Dallas memory button 79 to the unit 14 to lock the container 12. This data is communicated to the master database 20 where the records are updated. Thereafter, the second handler 28, who may be the same as or different from the first handler 24, transports the loaded container to the first remote location which, in the embodiment depicted in the drawings, is the exporting dock 30. Upon delivery, the master database 20 is once again updated. The handler 28 may access the master database 20 to retrieve selected status information or base line data, e.g. the location of container 12, from the master database 20. The status typically indicates whether or not the container 12 has been tampered with.

The export customs 48 also includes a PC 16 which is in communication with the master database 20. The export customs 48 also

has a Dallas memory button 79 for communicating transportation data between the unit 14, via its interface 78, and the PC 16. Appropriate codes may thus be communicated from the control centre 18 to the export customs 48 which may then be used to block or unblock or perform various other functions by transferring the code from the PC 16 to the unit 14 via the Dallas memory button 79.

Once the container 12 has been cleared by the export customs 48 it is then loaded onto the means of transport 32 which, in this case is typically a ship but may also be an aircraft or the like, it is transported to the destination docks 34. At the destination docks 34 the import customs 50 may retrieve transportation data from the unit 14 via a Dallas memory button 79 and the interface 78. The transportation data is then communicated to the PC 16 in a wireless fashion which then further communicates the data to the control centre 18 where the master database 20 is updated. The import customs 50 may thus obtain or retrieve status information on the container 12 from the database 20 and may selectively block the receiving client or importer 38 from opening the container 12 by communicating a "loaded container unlock" code into the controller 56 via the Dallas memory button 79. The "loaded container unlock code" prevents the container 12 from being opened even when the importer or receiving client 38 communicates his unique opening or unlock code to the unit 14.

Functions which the import customs 50 may perform include retrieving a bonded warehouse status of the container 12, uploading a bonded warehouse unlock block code, invoicing duties and printing financial statements via the PC 16, or the like. To enable the customs 50 to allow the importer or receiving client 38 to open the container 12, they

are also provided with a unique loaded container unblock code which unblocks the loaded container unlock code mentioned above thereby to enable the receiving client or importer 38 to open the container 12. Typically, in use, the customs official would then, once the container 12 has been delivered to the premises of the receiving client 38, send an official with the appropriate Dallas memory button 79 so that the container can be opened and the contents of the container 12 may be inspected in the presence of the importer or receiving client 38.

The container 12 is then transported from the docks 34 to the receiving or importing client 38 via the third handler 36. As is the case with all other intermediaries in the transportation process of the container 12 from the owner's depot 22 until it is finally delivered to the sub-depot 42 once the goods or cargo have been removed, all intermediaries may communicate with the control centre 18 and selectively access certain information in its database 20. Accordingly, each role player or intermediary may monitor the progress of the container during the transportation process.

The receiving client or importer 38 can retrieve at any time the status of the container 12 from the master database 20 and, as mentioned above, only the receiving client or importer 38 can retrieve data on the contents of the container 12.

Referring in particular to Figure 4 of the drawings, a more detailed representation is provided of communication between the various PCs 16 and the master database 20. Upon arrival of the container 12 at the docks 30 the transporter or handler 28 hands a status report to a customs official, or retrieves the status from the PC 16. The status report is

retrieved from the unit 14 via the Dallas memory button 79, as generally indicated by line 100. Thereafter, the customs official with his own Dallas memory button 79 retrieves further transportation data from the container 12 and downloads it via the Dallas memory button 79 to the PC 16. Typically, the aforementioned steps are executed at the time of arrival of the container 12 at the docks 30. Once the transportation data has been uploaded onto the PC 16 as shown by block 102, it is communicated via the PC 16 to the master database 20 as shown by line 104. The hardware provided at the dock 30 includes a printer and, once the transportation data has been uploaded into the PC 16, the PC 16 optionally prints out a status report and a copy thereof is handed to the transporter as proof of receipt of an untampered container as generally indicated in block 106. Prior to loading the container 12, a ship owner is provided with the printout of the status report as generally indicated by line 108. Thereafter, the status of container 12 is uploaded to the master database 20 as generally indicated by line 110. The same sequence of events is followed at the destination docks 34 as generally indicated by block 112. As mentioned above, the customs officials are selectively provided with unique identification devices including codes which empower them to block opening of the container 12 by the receiving or importing client 38 if the goods are not cleared, duty has not been paid, or for any other reason.

The system 10 typically provides a selection of different codes to the customs 48, 50 to allow them to control access to the container as mentioned above. In particular, customs officials may be provided with a facility to retrieve the status of any particular container 12, codes to block a "loaded container unlock code" provided to the importer 38, codes to unblock the "loaded container unlock code" e.g. upon a site visit, retrieve bonded warehouse status information for sample stock on hand,

appropriate codes which, via the Dallas memory button 79, upload "bonded warehouse" and unlock block codes, facilities to invoice duties which may be printable at a bonded warehouse, PC, or the like. Each service provider or role player at a remote location typically can receive or retrieve the status of a particular container, link with other role players, invoice debtors, or the like. The bonded warehouse may also include a PC 16 and Dallas memory button 79 to receive status data on the container 12, request customs officials to authorise unlocking of the container 12, link with customs as far as duty payments etc. are concerned, or the like. Clearing agents may also be provided with a PC 16 to obtain status data associated with a container 12, link with other role players, or the like. In a similar fashion, the insurer 44 may obtain status data on the container 12 and link with other role players.

It is however to be appreciated that any other data transfer unit (DTU) may be used. Hence, instead of the Dallas button 79, communication between the slave unit 14 and the exterior of the container can be by radio waves. In this embodiment, the communication interface 78 will be in the form of an antenna for transmitting and receiving signals. When the container is of a steel construction, difficulties can be encountered in the transmission of radio waves between the interior and the exterior of the container. The antenna will then typically be positioned adjacent to an opening which permits the transmission of radio waves. In this regard, the Inventor has found that a suitable opening is that provided by the hinges of the container doors in bulk transportation containers. Instead, a purpose made opening may be provided in the container.

Referring in particular to Figures 6 to 17 of the drawings, reference numeral 10.1 (see Figure 6) generally indicates a further embodiment of a

container management system in accordance with the invention. The container management system 10.1 substantially resembles the system 10 and, accordingly, like reference numerals have been used to indicate the same or similar features unless otherwise indicated.

The system 10.1 includes a control centre 18 with its master database 20 which is connected via a modem 150 to the Internet 152. Each remote unit 16 of the system 10.1 also includes a modem 154 for connecting the remote unit 16 to the Internet 152. The remote unit 16 optionally includes a variety of different interfaces or communication means for communicating with a slave unit 14 mounted in a container 12. In particular, the remote unit 16 may include any conventional data transfer unit (DTU) interface 156, a radio frequency (RF) interface 158, or the like. Accordingly, the slave unit 14 may include an RF interface 160 for communication with the RF interface 158, or a corresponding DTU interface 162 for communicating with the DTU interface 156. The DTU interfaces 156, 162 and RF interfaces 158, 160 allow wireless communication between the slave unit 14 and the remote unit 16. In the system 10.1, data may be downloaded from the master database 20 to each slave unit 14 as generally indicated by arrow 164 and uploaded in a reverse direction from the slave unit 14 to the master database 20 as generally indicated by arrow 166.

The system 10.1 includes an identification interface 168 for identifying an operator or user involved in the system 10.1. Status information of the container 12 may be uploaded from the slave unit 14 via its RF interface 160 to the RF interface 158 and fed into the remote unit 16. Thereafter, the status information may be communicated via the Internet 152 to the control centre 18 where its master database 20 may be

updated. When data is communicated between the master database 20, the remote unit 16 and the slave unit 14 the operator involved may thus be identified.

The identification interface 168 uniquely identifies the operator or user and may include any conventional identification means such as fingerprint identification, thumbprint identification, a retina scanner, a transponder-like device operable to identify a corresponding tag carried by the operator, voice recognition, or the like. Thus no visible recognition code or the like need be entered to reduce the likelihood of unauthorised access. The recognition code may change with time.

Each user or operator may be provided with selected access rights which may be defined in the master database 20. Accordingly, once an operator identifies himself via the identification interface 168, the control centre 18 may inspect its master database 20 and selectively allow or disallow various requests submitted by the operator via the remote unit 16. If the operator is however authorised with or assigned particular access rights, the control centre 18 would then instruct the remote unit 16 and slave unit 14 accordingly by downloading information as shown by the arrow 164. Thus, lock, unlock, arm, disarm, or any other commands may be downloaded from the control centre 18 via the Internet 152 to the remote unit 16. The remote unit 16 may then communicate the data in a wireless fashion to the slave unit 14.

As shown in Figure 7, communication between the control centre 18 and remote and slave units 16, 14 respectively, need not be via a hardwired communication link but may use satellite technology. Accordingly, the slave and remote units 14, 16 and the control centre 18

may include satellite dishes 170 with associated electronics for communicating with a satellite 172.

The control centre 20 of the system 10.1 includes control software 174 (see Figure 8) which controls the storage and retrieval of transportation and management data from the database 20. Typically, the database 20 includes client data 176 e.g. the access rights within a particular company, status data 178 e.g. is the container okay or has it been tampered with, and transaction data 180 e.g. the route information, the access rights to various parties, whether or not there is a customs block on the container 12, is the container 12 bonded, in whose custody is the container, who will be the next custodian of the container, and so on.

The control centre 18 further includes a web site 182 and a web front end 184 for interfacing the web site 182 to the control software 174. Staff at the control centre (generally indicated by reference numeral 186) may enter and modify data using the software 174. The modem 150 links the control centre to an appropriate Internet service provider.

In certain embodiments of the remote unit 16, the personal computer is linked via the modem 154 via a hardwired telephone line 188 (see Figure 9) to a further modem 190 provided at a service provider 192. The service provider 192 is linked to the Internet 152. The remote unit 16 includes the RF and DTU interfaces 158, 156 respectively for communicating with the slave unit 14 in a wireless fashion. The identification interface 168 may use any conventional identification means to identify the operator including voice recognition or the like, as mentioned above.

Comprehensive details on the slave unit 14 are automatically registered in the master database 20 when the container 12 is fitted with the slave unit 14 (see Figure 10). Comprehensive registration details may be communicated via the slave unit 14 in a wireless fashion to the remote unit 16 which, in turn, communicates the data to the master database 20 as hereinbefore described. Alternatively, an installer 194 may communicate the unique identification data of the slave unit 14 to the control centre 18 upon installation. Typically, a unique serial number of each slave unit 14, as well as comprehensive details on an owner who has purchased the slave unit 14, are entered into the master database 20 either via the Internet or telephonically.

When a client requests a container 12 fitted with the slave unit 14, the client, via its remote unit 16, identifies himself to the control centre 18 as shown by arrow 196 (Figure 11). A container 12 is then ordered and transaction data is completed on the web site 182. Typical transaction data includes details on the intermediate handlers of the container 12 and the control centre 18 then assigns lock and unlock rights to various employees of the client. Thus, various parties or employees at various destination points along which the container 12 is transported may be uniquely identified and each allocated unique access rights. Typically, when a client requests a container 12 transaction data including route data, the various parties who will handle the container 12 being transported, various clients, driver routing instructions, or the like may be uploaded into the master database 20.

Once a container 12 has been requested, a container 12 is assigned to a transaction at the owner's depot (see Figure 12). After receiving an order for the container 12, the container owner 22 services

the container 12 and assigns it to the appropriate transaction after he has identified himself by means of the identification interface 168 as shown by arrow 198. Thereafter, the control centre 18 requests the status of the container as shown by arrows 200. In response to the request, the slave unit 14 communicates its status via arrows 202 to the control centre 18 and, in response thereto, the master database 20 is updated. Once the data has been verified, the control centre 18 then downloads lock and arm commands to the slave unit 14 as shown by arrows 204. The slave unit 14 then locks and arms the container 12 and, once this has been completed, communicates an updated status to the control centre 18 as shown by arrows 206. Thus, prior to despatching the container 12 to a depot, the container 12 is first serviced and closed and the appropriate commands are communicated to the slave unit 14.

As the container 12 is transported to various locations and, finally, to its destination location custodianship of the container 12 is passed on to the various handlers or clients (see Figure 13). In particular, when a container 12 is delivered, the new handler identifies himself via the remote unit 16 and its identification interface 168 (see Figure 9) and requests transferral of custodianship from the control centre 18. In particular, if the container 12 is being delivered, then the recipient handler communicates with the control centre 18 from his remote unit 16. However, if the container 12 is being collected, the handler passing on custodianship communicates via his remote unit 16 to the control centre 18.

The control centre 18 then verifies the status of the slave unit 14 and communicates with the remote unit 16 which then advises or records that custodianship has been transferred. Typically, a message appears on a monitor of the PC indicating that custodianship has been transferred

from party A to party B. Once custodianship has been transferred and recorded, the new handler is responsible for the container 12. The arrow 208 indicates identification by the new handler, and arrows 210 show communication between the control centre 18 and the slave unit 14 for monitoring status, for showing a change in custodianship has been recorded, or the like.

When access to the container 12 is required at one of the destination points along the transportation route or at its destination as the case may be, the client first identifies himself to the system 10.1 and requests that the container be unlocked as shown by arrow 212 (see Figure 14). The control centre 18 then verifies the particular access rights of the person identified and requests status data from the slave unit 14 as generally indicated by arrows 214. The slave unit 14 then communicates the requested data which is then uploaded into the master database 20 as shown by arrows 216. If the control centre is satisfied that the status data is acceptable, then an unlock command is downloaded into the slave unit 14 as shown by arrows 218 and further status data from the slave unit 14 is then uploaded as shown by arrows 220. The goods may then be removed from the container 12 whereafter the client identifies himself and requests that the container 12 be locked as generally indicated by arrow 222. The control centre 18 then downloads a lock command as shown by arrow 224 which is reacted upon by the slave unit 14 which then locks the container 12. After the container has been locked, its status is uploaded into the master database 20 as shown by arrow 226.

Referring in particular to Figure 15 of the drawings, the container 12 may be bonded/unbonded, access thereto may be blocked or unblocked by customs, or the like. In particular, customs officials identify themselves

via their remote unit 16 which communicates identification data (see arrow 228) to the control centre 18 whereupon its master database 20 is updated. The customs officials request a block, bond, or other command be placed or removed from the container 12 and, in response thereto, the control centre 18 communicates with the slave unit 14 in a similar fashion as hereinbefore described. It is however to be appreciated that not only customs officials can bond or unbond a container 12 but that any handler may restrict further movement of the container 12. If, for example, the recorded status of the container is that the container has been tampered with, then a handler may refuse to accept custodianship of the container and enters his refusal in the database. All affected parties can then investigate the matter.

The slave unit 14 itself is not aware of the bonding or unbonding, blocking or unblocking but the status thereof is stored in the master database 20. However, in the case of a grounded container 12, the slave unit 14 may be periodically monitored as generally indicated by arrows 230 by means of the wireless RF interface to sense or monitor movement of the container 12. If movement is detected, the remote unit 16 may then trigger the appropriate alarms.

In order to unlock a blocked or bonded container, the client identifies himself by means of the remote unit 16 and communicates a request for an unlock code from the control centre 18 as shown by arrow 232 (see Figure 16). The control centre 18 then inspects its master database 20 to verify that a block or bond has been placed on the container 12 and then requests the customs official to identify himself at the client's remote unit 16 as shown by arrow 234. A similar communication method is then followed as generally indicated by arrows

214, 216, 218, 220, 222, 224, and 226 as shown in Figure 14. Further, it is to be appreciated that additional communication routines may be followed when carrying out various requests or functions.

Referring in particular to Figure 17 of the drawings, a client/handler is automatically registered when the remote unit 16 peripherals are installed at his site. Selected employees are identified by the client and issued with identification devices, their fingerprints may be taken, or any other identification means may be employed to identify the employees via the identification interface 168. Thus, each time an employee uses the system 10.1 he may be identified and various access rights may be assigned to him. Further, it is to be appreciated that in different embodiments of the invention passwords or the like may be stored in the master database 20 and/or the slave unit 14. In a preferred embodiment, the passwords or unique identifiers are preferably defined in the master database 20 and downloaded into the slave unit 14 which then has storage means for storing the data. Further, it is to be appreciated that the system 10, 10.1 may be included in all forms of road, rail, and air transport vehicles and trailers to monitor and manage the transportation of goods. For example, the container 12 may be an open container such as a rail vehicle where access is provided through doors. In addition, pantechnicons or the like which transport goods via road may include a slave unit 14 to manage transportation of goods.

A variety of different functions and activities may be monitored using the system 10, 10.1. For example, each time the container 12 is armed a time stamp may be communicated to the main database 20, likewise, when the container is locked, grounded, bonded, blocked, power level is low, status of the peripherals within the container, or the like may

be monitored and date and time stamps may be effected periodically. Further, by means of the identification interface 168, operators dealing with the container 12 are identified and a record thereof may be kept.

It will be appreciated that the invention has been described above with reference to a lockable container. However, the Inventor believes the invention will also find application for example in the transportation of hazardous chemicals where another or an additional parameter, eg temperature inside the container, may be monitored. This arrangement permits the transportation of the container to be managed and ensures that the responsible person is informed should the monitored parameter fall outside predetermined limits.

The Inventor believes that the invention, as illustrated, provides a method and system for the management of the transportation of goods containers which facilitates monitoring and managing the transportation of containers 12 from an exporter 26 to an importer 38. As relevant transportation data is sourced from the container 12 at each remote location along its route, the database 20 may be updated to include comprehensive details on the progress of the container to its destination. Further, a mapped route may be provided in the database 20 against which progress of the container 12 may be verified. As none of the intermediaries are provided with information on the contents of the container 12 the likelihood of theft is reduced. Further, access to each container 12 is controlled by a unique identification code thereby enhancing security of the contents of the container 12. The Inventor further believes that it is an advantage of the invention that the container 12 is locked from within and, therefore, does not have an exposed locking arrangement which may be tampered with.

The Inventor further believes that administration will be greatly simplified. For example, in view of the fact that the supplier enters all details of goods loaded, invoice details, payment instructions, customs information etc., the only paperwork required at the suppliers base is the delivery and destination details. Invoices can be printed out by the receiver via the Internet access to the database. Payments can be electronically transferred via the Internet and recorded in the database. A suppliers unlock/block code can be entered if invoices are not paid. This results in a great reduction in the paperwork associated with the transportation of goods. Further, dock congestion can be avoided by customs officials applying a block code permitting a container to be despatched to its final destination at which the contents can be investigated. Customs officials further benefit by being sure that a complete untampered consignment arrives at the final destination thereby being assured of full customs duty. Insurers have improved protection since they can pinpoint at which custodian tampering took place and as a result who is liable for any losses which may then have been incurred. Further, law enforcement agencies are assisted in being able to pinpoint the place and time of tampering.

CLAIMS

1. A container which includes

a body defining a goods receiving cavity within which goods are receivable, the body having an access opening through which goods can be introduced into and removed from the cavity;

a closure element for closing the access opening;

a lock for locking the closure element releasably in a closed position; and

a lock actuator for displacing the lock between a locked position and an unlocked position, the lock actuator being positioned inside the container body and having an interface for communicating with a remote controller positioned outside the container.

2. A container as claimed in claim 1, which includes a container slave unit at least part of which is mounted within the body for monitoring data relating to the container, the lock actuator forming part of the slave unit.

3. A container as claimed in claim 2, in which the slave unit includes a power source and in which at least part of the slave unit is dismountably mounted in the container.

4. A container as claimed in claim 2 or claim 3, in which the slave unit includes a transmitter and a receiver for communicating in a wireless fashion with a remote controller having a complementary transmitter and receiver.

A container as claimed in claim 4, in which the slave unit includes an antenna to permit communication with a remote controller by radio wave.

6. A container as claimed in claim 5, in which the antenna is positioned within the container body contained in a casing which serves to protect the antenna and resist tampering therewith.

7. A container as claimed in claim 6, which includes a transmission opening adjacent to which the antenna is positioned.

8. A container as claimed in any one of claims 2 to 7, inclusive, in which the slave unit includes a unique identifier, uniquely to identify the container within which it is mounted.

9. A container as claimed in any one of the preceding claims, which includes tamper detection means for monitoring tampering with the container.

10. A container as claimed in claim 9, in which the tamper detection means includes a light sensor for sensing light within the container.

11. A container as claimed in claim 9 or claim 10, in which the tamper detection means includes a movement sensor sensing unauthorised movement of the container.

12. A container as claimed in any one of claims 9 to 11, inclusive, which includes an alarm responsive to the tamper detection means for generating an audible alarm.

13. A container as claimed in any one of the preceding claims, which includes repelling means for repelling an unauthorised entry into the container.

14. A container as claimed in claim 13, in which the repelling means includes an atmospheric induction unit for releasing a chemical substance in the container.

15. A container as claimed in any one of the preceding claims, which includes a tracking device for tracking the geographical position of the container.

16. A container management system for managing transportation of containers, the system including

at least one container;

a container slave unit mounted to the container for monitoring data relating to the container;

a plurality of remote units provided at selected remote locations to which the container is to be transported, each remote unit being operable to communicate with the container slave unit to retrieve data from the slave unit; and

a control centre including a master database for storing management data relating to the container, the control centre being connected to connectable in communication with each remote unit to receive the data from the container slave unit and thereby update the management data.

17. A container management system as claimed in claim 16, in which the container slave unit also monitors transportation data and functions to control access to the container.

18. A container management system as claimed in claim 16 or claim 17, in which the control centre includes comparator means for comparing data sourced from each remote unit with data stored on the master database for generating a warning signal or alarm condition if the comparison indicates an excessive deviation from the master database .

19. A container management system as claimed in any one of claims 16 to 18, inclusive, in which the slave unit includes an electrically operable locking arrangement for controlling access to the container.

20. A container management system as claimed in claim 19, in which the locking arrangement is mounted within the container.

21. A container management system as claimed in any one of claims 16 to 20, inclusive, in which communication between the slave unit and each remote unit is done in a wireless fashion.

22. A container management system as claimed in any one of claims 16 to 20, inclusive, in which communication between the slave unit and each remote unit is by radio wave, the slave unit then including an antenna.

23. A container management system as claimed in claim 22, in which the antennae is mounted within the container and encapsulated within a protective material which does not interfere with radio transmission.

24. A container management system as claimed in any one of claims 16 to 23, inclusive, in which the slave unit is mounted within the container and includes tamper detection means for monitoring tampering with the container.

25. A container management system as claimed in claim 24, in which the tamper detection means includes a light sensor for sensing light within the container.

26. A container management system as claimed in claim 24 or claim 25, in which the detection means includes a movement sensor for sensing unauthorised movement of the container.

27. A container management system as claimed in any one of claims 24 to 26, inclusive, in which the slave unit includes an internal movement sensor.

28. A container management system as claimed in any one of claims 24 to 27, inclusive, in which the slave unit includes an impact sensor.

29. A container management system as claimed in any one of claims 24 to 28, inclusive, in which the slave unit includes an alarm responsive to the tamper detection means and/or the movement sensor for generating an audible alarm.

30. A container management systems as claimed in any one of claims 16 to 29, inclusive, in which the slave unit includes repelling means for repelling an unauthorised entry into the container.

31. A container management system as claimed in claim 30, in which the repelling means includes an atmospheric induction unit for releasing a chemical substance in the container.

32. A container management system as claimed in any one of claims 16 to 31, inclusive, in which the slave unit is a microprocessor based unit including storage means for storing at least the transportation data for communication to the remote unit.

33. A container management system as claimed in claim 32, in which the slave unit is arranged to log or record a plurality of events relating to the container

34. A container management system as claimed in any one of claims 16 to 33 inclusive, in which the slave unit includes its own power source.

35. A container management system as claimed in any one of claims 16 to 34, inclusive, in which the slave unit includes a tracking device for tracking the geographical position of the container.

36. A container management system as claimed in any one of claims 16 to 35, inclusive, in which the slave unit includes a sleep mode.

37. A container management system as claimed in any one of claims 16 to 36, inclusive, which includes a plurality of containers each having slave unit which has a unique identifier, uniquely to identify the container within which it is mounted.

38. A container management system as claimed in any one of claims 16 to 37, inclusive, in which at least a part of the container slave unit is dismountably mounted to the container.

39. A method of controlling access to a container, the method including

providing a container slave unit in the container which slave unit is operable to provide transportation and access data relating to the container;

communicating transportation and access data between the slave unit and a remote unit at an associated remote location between a supplier of goods transported in the container and a receiver of the goods;

communicating transportation and access data between the remote unit and a control centre; and

verifying the transportation data to determine if unauthorised access to the container has occurred.

40. A method as claimed in claim 39, which includes contolling access to the container by verifying transportation data to determine if access to the container should be permitted, and if so, communicating an access code to the remote unit for communication to the slave unit thereby selectively to allow access to the container.

41. A method of managing the transportation of goods from a supplier to a receiver in a container provided with a slave unit for monitoring data relating to the container, which method includes

retrieving data from the slave unit at selected locations; and

comparing the retrieved data with data stored on a master database to check on the status of the container.

42. A method as claimed in claim 41, which includes the prior step of entering data in the master database at a control centre, comparing the retrieved data with the data on the database including communicating the retrieved data from the or each selected location to the control centre, the method further including updating the data on the master database.

43. A method as claimed in claim 41 or claim 42, in which at least part of the slave unit is mounted inside the container and data from the slave unit is retrieved in a wireless fashion.

44. A slave unit which is mountable in a lockable enclosure, the slave unit including

a controller for receiving data relating to a said lockable enclosure in which it is mounted; and

a communication interface for communication with a remote unit having a complementary communication interface.

45. A slave unit as claimed in claim 44, which includes lock control means for controlling the operation of the lock of a lockable enclosure in which the slave unit is mounted.

46. A container as claimed in claim 1, substantially as described and illustrated herein.

47. A container management system as claimed in claim 16, substantially as described and illustrated herein.

48. A method of controlling access to a container as claimed in claim 38, substantially as described and illustrated herein.

49. A method of managing the transportation of goods as claimed in claim 41, substantially as described and illustrated herein.

50. A slave unit as claimed in claim 44, substantially as described and illustrated herein.

51. A new container, system, method or slave unit substantially as described herein.

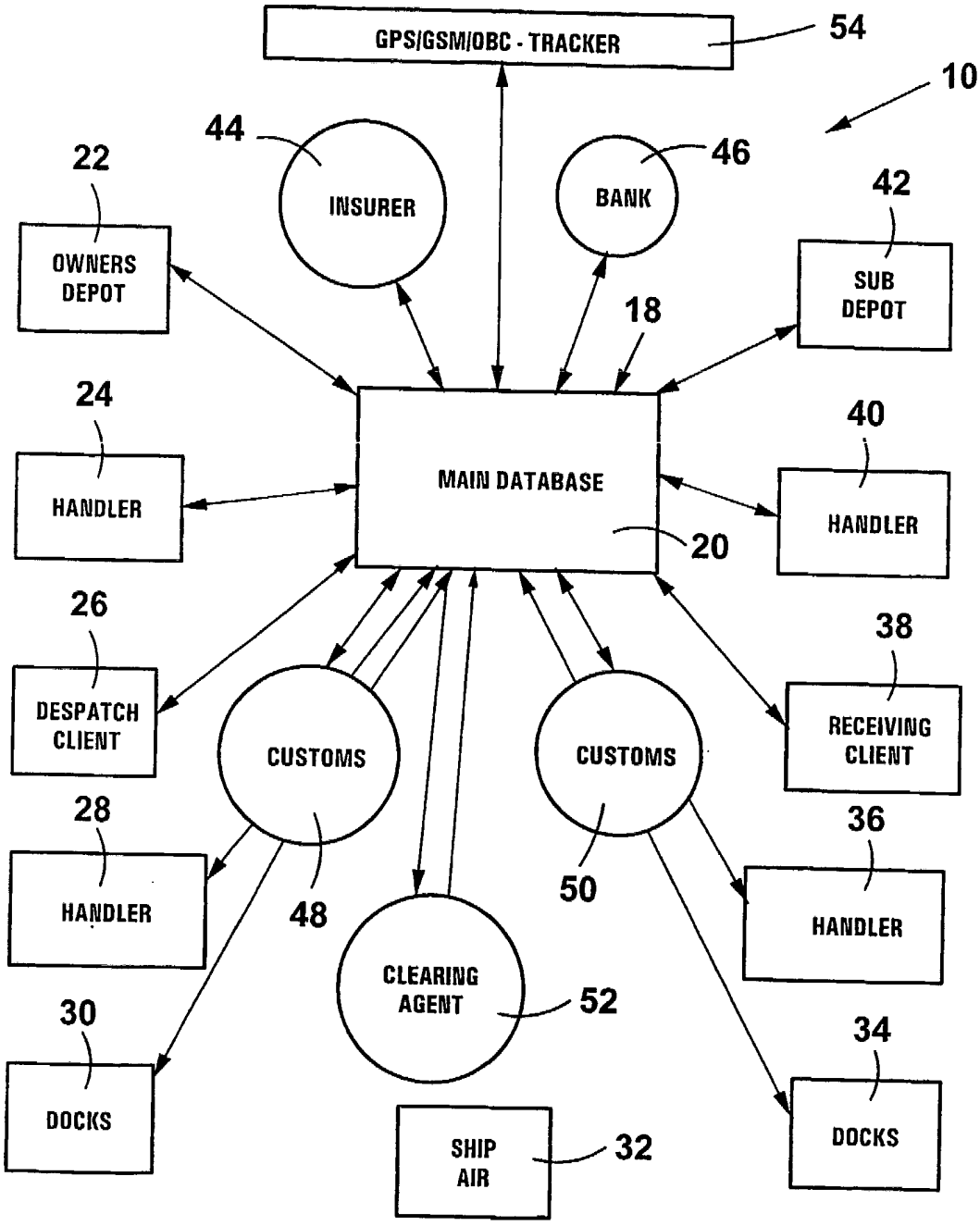

GPS/GSM/OBC - TRACKER
54
10
44
INSURER
46
BANK
22
OWNERS DEPOT
42
SUB DEPOT
18
24
HANDLER
MAIN DATABASE
40
HANDLER
20
26
DESPATCH CLIENT
CUSTOMS
CUSTOMS
38
RECEIVING CLIENT
28
HANDLER
48
50
36
HANDLER
CLEARING AGENT
52
30
DOCKS
34
DOCKS
SHIP AIR
32

FIG 1

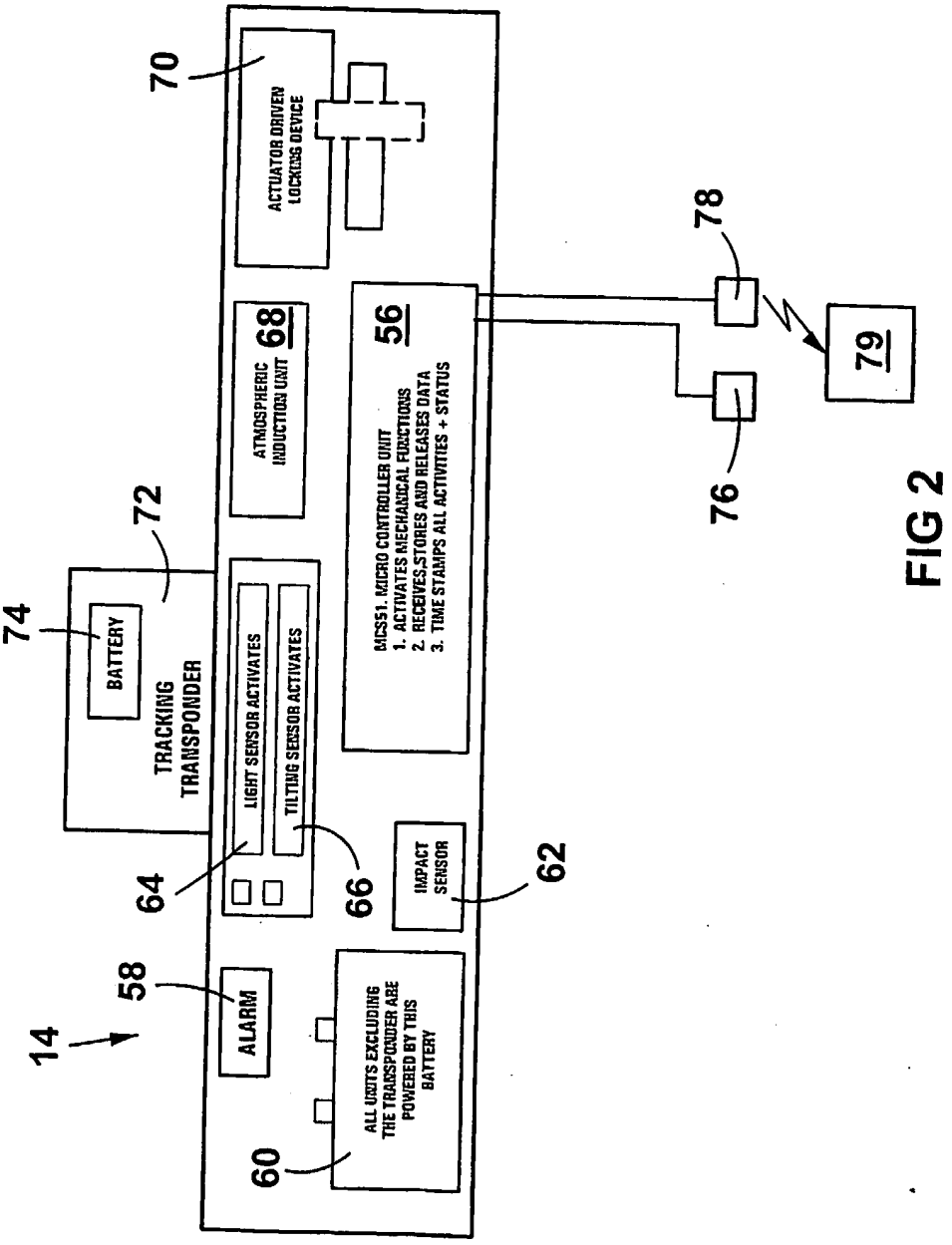

70
ACTUATOR DRIVEN LOCKING DEVICE
78
ATMOSPHERIC INDUCTION UNIT 68
56
MICS1. MICRO CONTROLLER UNIT
1. ACTIVATES MECHANICAL FUNCTIONS
2. RECEIVES,STORES AND RELEASES DATA
3. TIME STAMPS ALL ACTIVITIES + STATUS
79
76
72
74
BATTERY
TRACKING TRANSPONDER
LIGHT SENSOR ACTIVATES
TILTING SENSOR ACTIVATES
64
66
IMPACT SENSOR
62
58
14
ALARM
ALL UNITS EXCLUDING THE TRANSPONDER ARE POWERED BY THIS BATTERY
60

FIG 2

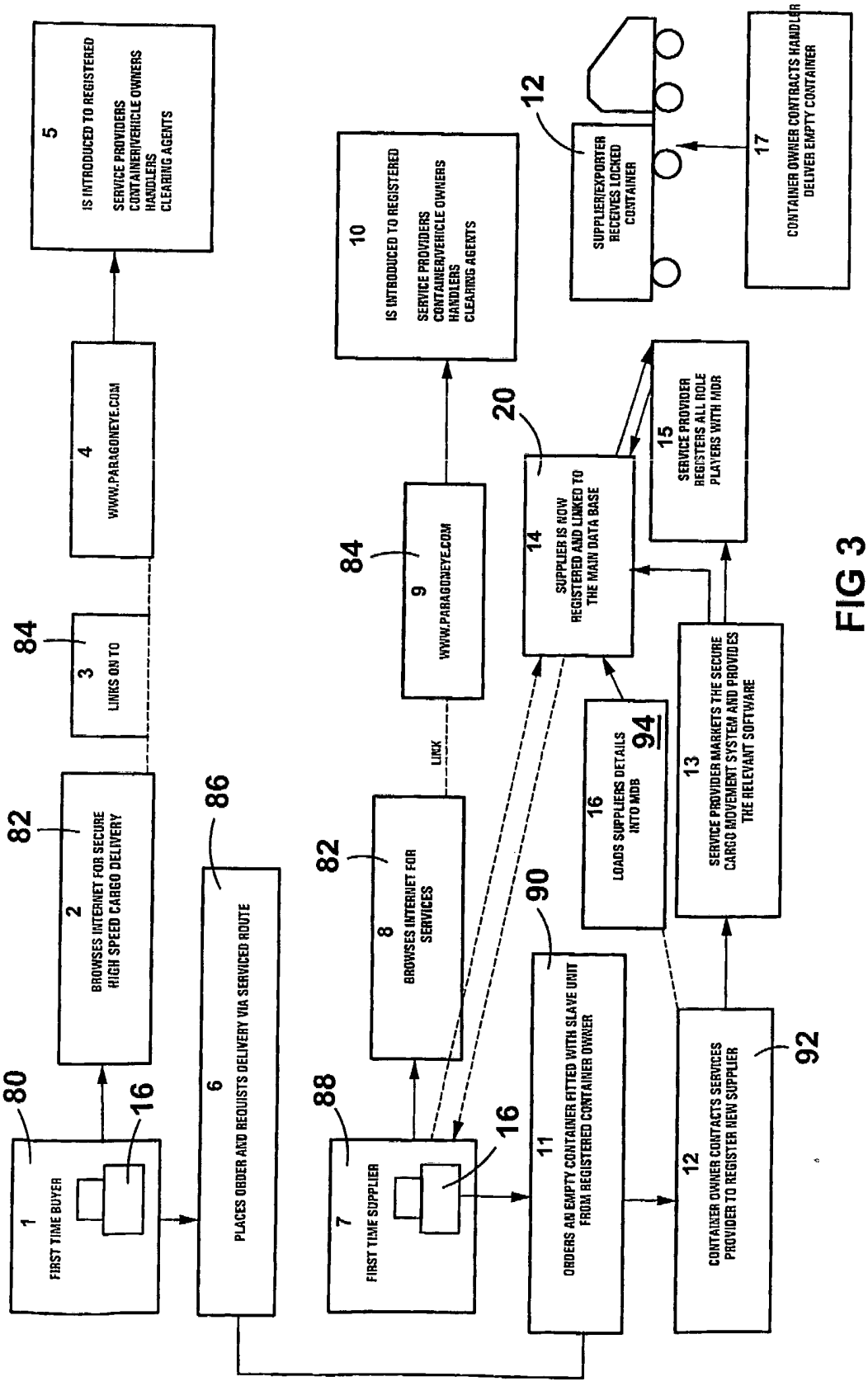

1 FIRST TIME BUYER
2 BROWSES INTERNET FOR SECURE HIGH SPEED CARGO DELIVERY
3 LINKS ON TO
4 WWW.PARAGONEYE.COM
5 IS INTRODUCED TO REGISTERED SERVICE PROVIDERS CONTAINER/VEHICLE OWNERS HANDLERS CLEARING AGENTS
6 PLACES ORDER AND REQUISTS DELIVERY VIA SERVICED ROUTE
7 FIRST TIME SUPPLIER
8 BROWSES INTERNET FOR SERVICES
9 WWW.PARAGONEYE.COM
10 IS INTRODUCED TO REGISTERED SERVICE PROVIDERS CONTAINER/VEHICLE OWNERS HANDLERS CLEARING AGENTS
11 ORDERS AN EMPTY CONTAINER FITTED WITH SLAVE UNIT FROM REGISTERED CONTAINER OWNER
12 CONTAINER OWNER CONTACTS SERVICES PROVIDER TO REGISTER NEW SUPPLIER
12 SUPPLIER/EXPORTER RECEIVES LOCKED CONTAINER
13 SERVICE PROVIDER MARKETS THE SECURE CARGO MOVEMENT SYSTEM AND PROVIDES THE RELEVANT SOFTWARE
14 SUPPLIER IS NOW REGISTERED AND LINKED TO THE MAIN DATA BASE
15 SERVICE PROVIDER REGISTERS ALL ROLE PLAYERS WITH MDB
16 LOADS SUPPLIERS DETAILS INTO MDB 94
17 CONTAINER OWNER CONTRACTS HANDLER DELIVER EMPTY CONTAINER
16
16
80
82
84
86
88
90
92
20
LINK

FIG 3

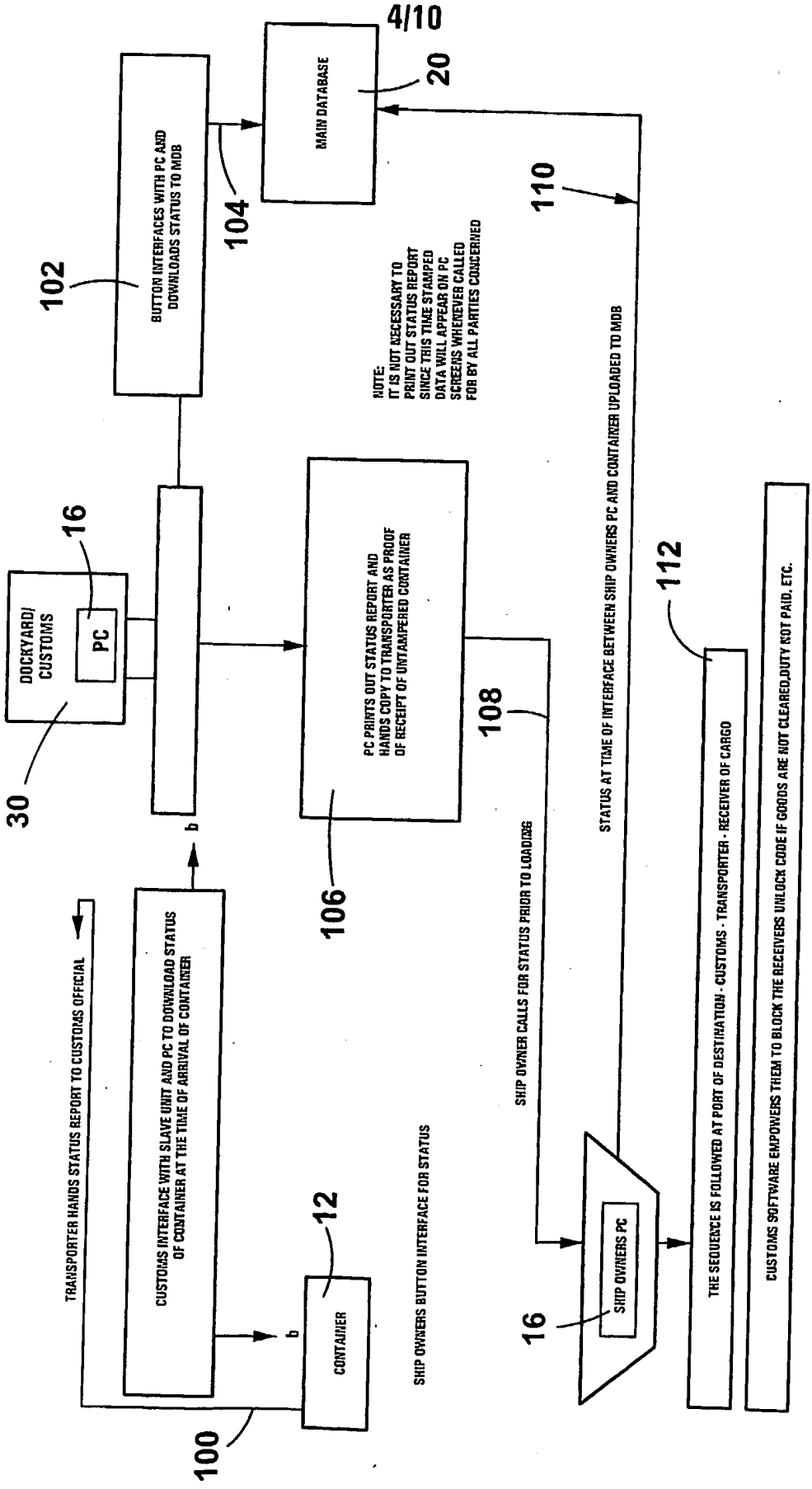

MAIN DATABASE
20
BUTTON INTERFACES WITH PC AND DOWNLOADS STATUS TO MDB
102
104
110
NOTE:
IT IS NOT NECESSARY TO PRINT OUT STATUS REPORT SINCE THIS TIME STAMPED DATA WILL APPEAR ON PC SCREENS WHENEVER CALLED FOR BY ALL PARTIES CONCERNED
DOCKYARD/ CUSTOMS
PC
16
30
PC PRINTS OUT STATUS REPORT AND HANDS COPY TO TRANSPORTER AS PROOF OF RECEIPT OF UNTAMPERED CONTAINER
106
108
STATUS AT TIME OF INTERFACE BETWEEN SHIP OWNERS PC AND CONTAINER UPLOADED TO MDB
112
CUSTOMS INTERFACE WITH SLAVE UNIT AND PC TO DOWNLOAD STATUS OF CONTAINER AT THE TIME OF ARRIVAL OF CONTAINER
TRANSPORTER HANDS STATUS REPORT TO CUSTOMS OFFICIAL
CONTAINER
12
100
SHIP OWNERS BUTTON INTERFACE FOR STATUS
SHIP OWNER CALLS FOR STATUS PRIOR TO LOADING
SHIP OWNERS PC
16
THE SEQUENCE IS FOLLOWED AT PORT OF DESTINATION - CUSTOMS - TRANSPORTER - RECEIVER OF CARGO
CUSTOMS SOFTWARE EMPOWERS THEM TO BLOCK THE RECEIVERS UNLOCK CODE IF GOODS ARE NOT CLEARED,DUTY NOT PAID, ETC.

FIG 4

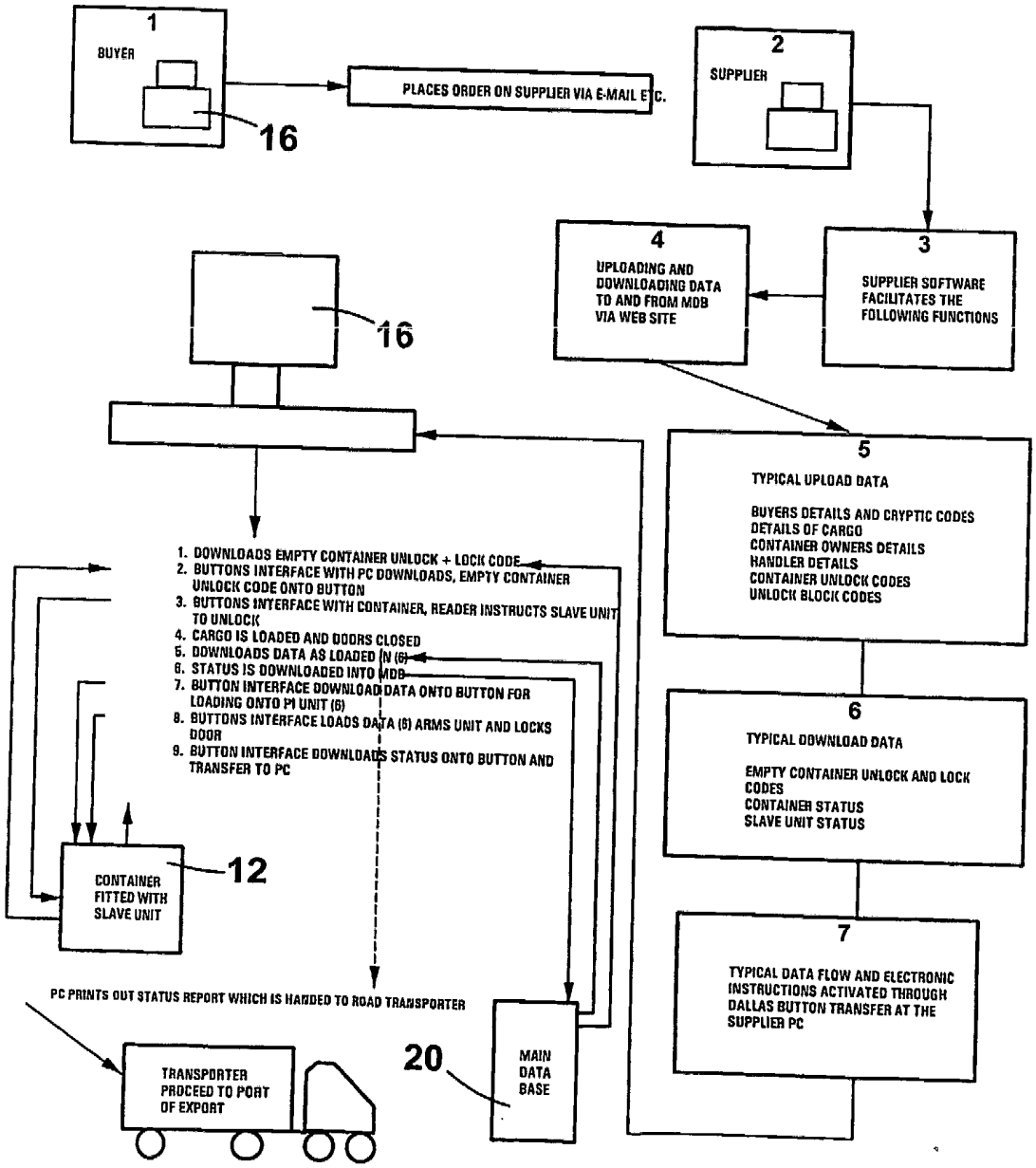

1
BUYER
16
PLACES ORDER ON SUPPLIER VIA E-MAIL ETC.
2
SUPPLIER
4
UPLOADING AND DOWNLOADING DATA TO AND FROM MDB VIA WEB SITE
3
SUPPLIER SOFTWARE FACILITATES THE FOLLOWING FUNCTIONS
16
5
TYPICAL UPLOAD DATA
BUYERS DETAILS AND CRYPTIC CODES
DETAILS OF CARGO
CONTAINER OWNERS DETAILS
HANDLER DETAILS
CONTAINER UNLOCK CODES
UNLOCK BLOCK CODES
1. DOWNLOADS EMPTY CONTAINER UNLOCK + LOCK CODE
2. BUTTONS INTERFACE WITH PC DOWNLOADS, EMPTY CONTAINER UNLOCK CODE ONTO BUTTON
3. BUTTONS INTERFACE WITH CONTAINER, READER INSTRUCTS SLAVE UNIT TO UNLOCK
4. CARGO IS LOADED AND DOORS CLOSED
5. DOWNLOADS DATA AS LOADED IN (6)
6. STATUS IS DOWNLOADED INTO MDB
7. BUTTON INTERFACE DOWNLOAD DATA ONTO BUTTON FOR LOADING ONTO PI UNIT (6)
8. BUTTONS INTERFACE LOADS DATA (6) ARMS UNIT AND LOCKS DOOR
9. BUTTON INTERFACE DOWNLOADS STATUS ONTO BUTTON AND TRANSFER TO PC
6
TYPICAL DOWNLOAD DATA
EMPTY CONTAINER UNLOCK AND LOCK CODES
CONTAINER STATUS
SLAVE UNIT STATUS
12
CONTAINER FITTED WITH SLAVE UNIT
7
TYPICAL DATA FLOW AND ELECTRONIC INSTRUCTIONS ACTIVATED THROUGH DALLAS BUTTON TRANSFER AT THE SUPPLIER PC
PC PRINTS OUT STATUS REPORT WHICH IS HANDED TO ROAD TRANSPORTER
TRANSPORTER PROCEED TO PORT OF EXPORT
20
MAIN DATA BASE

FIG 5

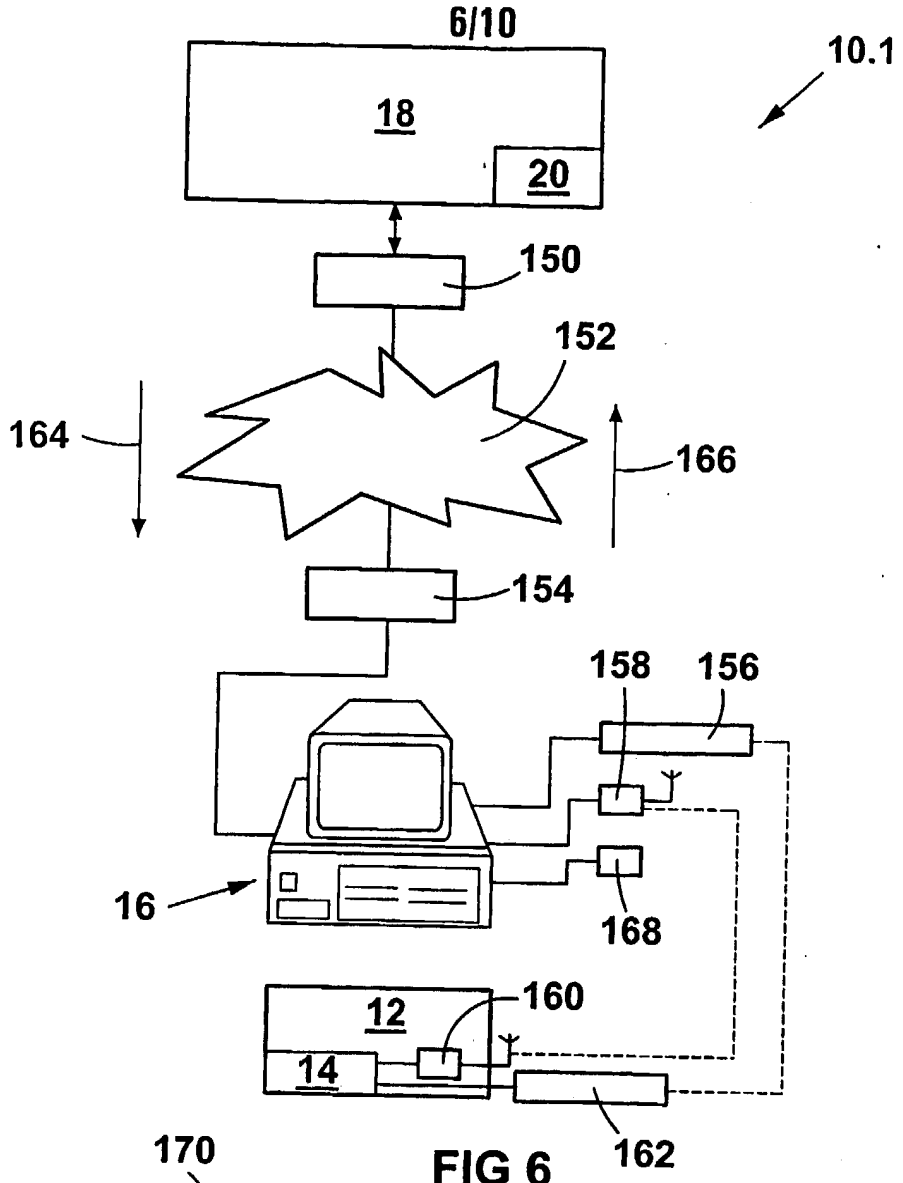

10.1
18
20
150
152
164
166
154
158
156
16
168
12
160
14
162

FIG 6

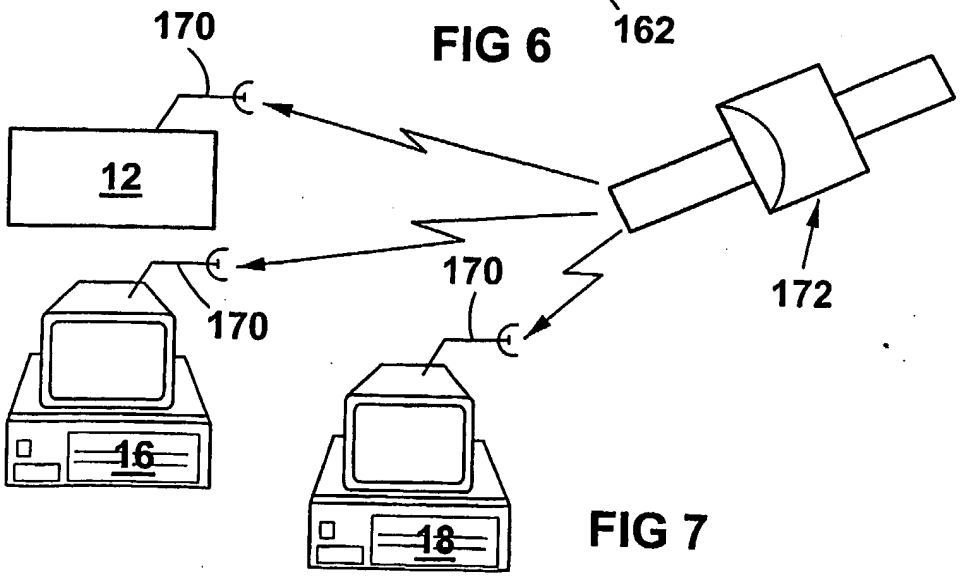

170
12
172
170
170
16
18

FIG 7

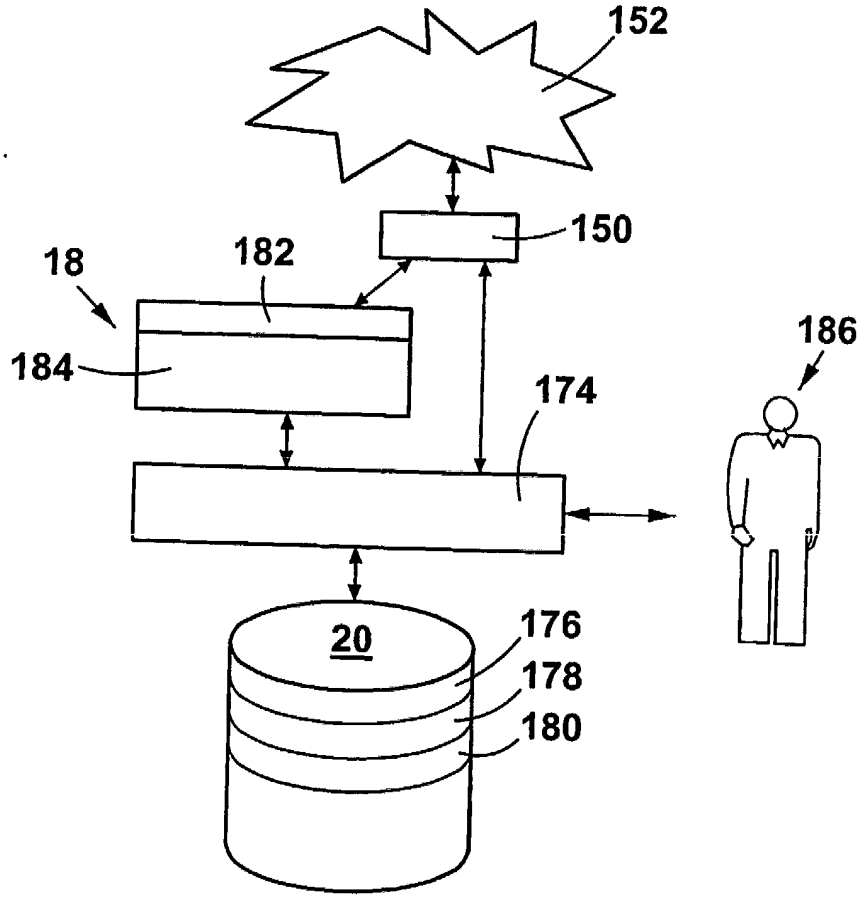

152
150
18
182
184
186
174
20
176
178
180

FIG 8

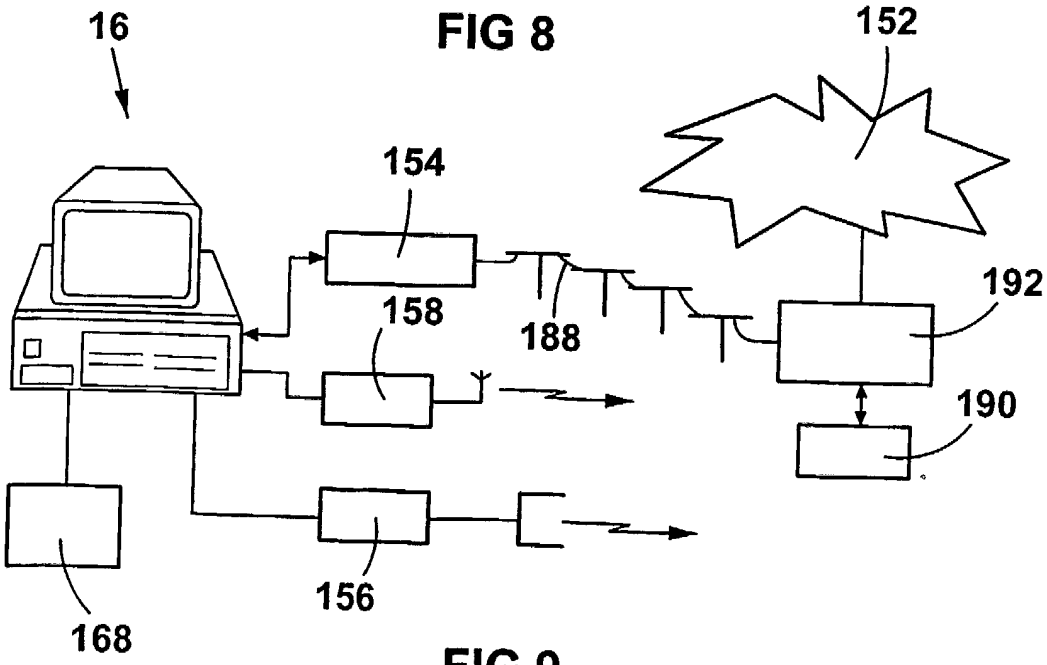

16
152
154
158
188
192
190
168
156

FIG 9

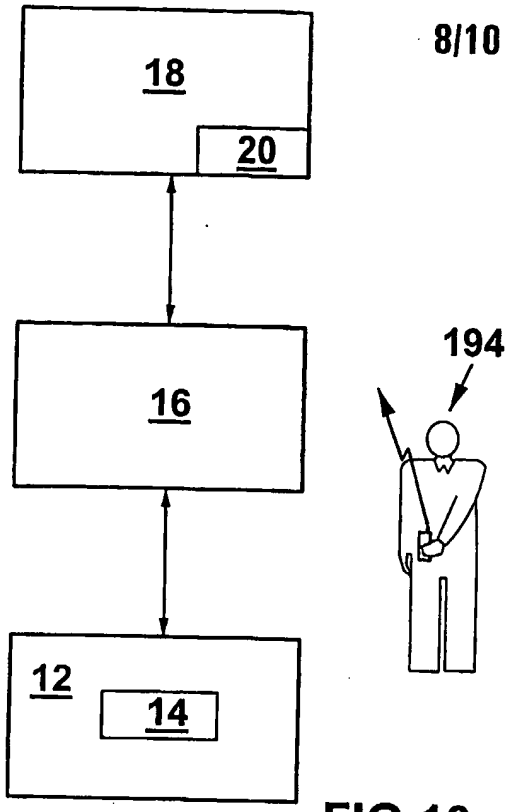
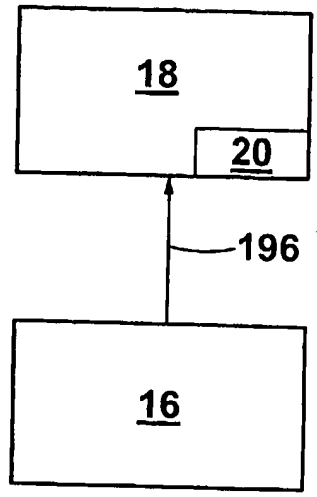


FIG 10



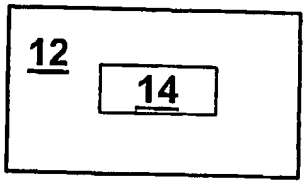


FIG 11

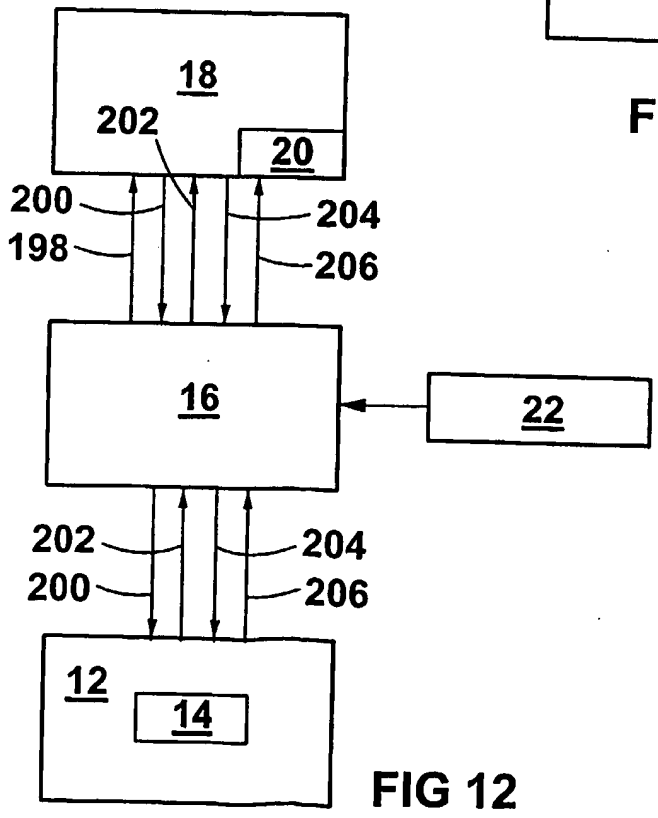


FIG 12

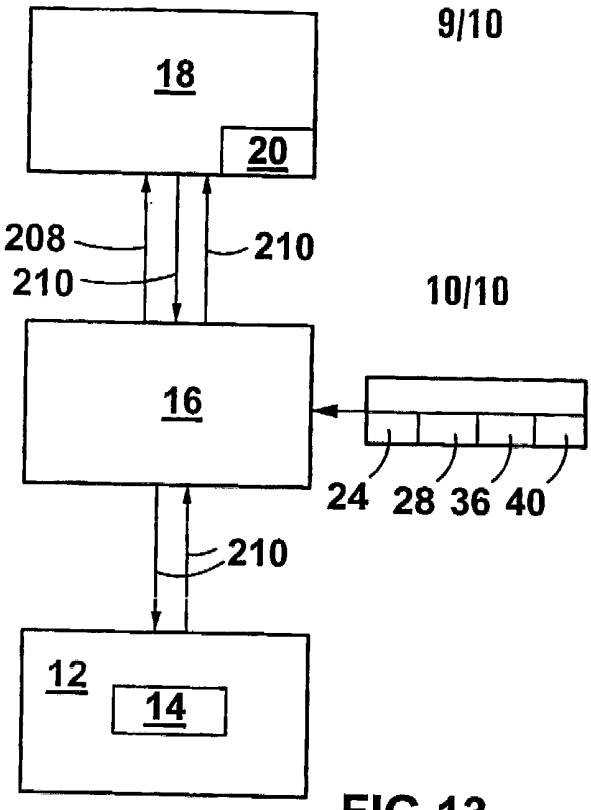


FIG 13

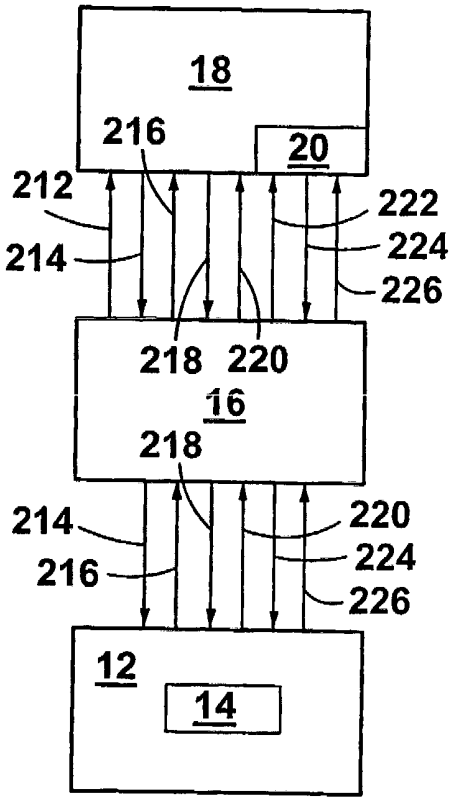


FIG 14

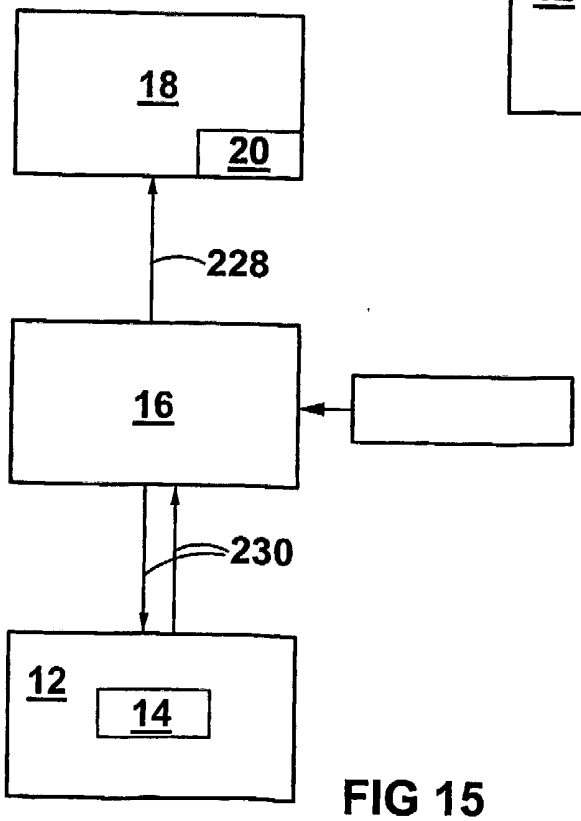
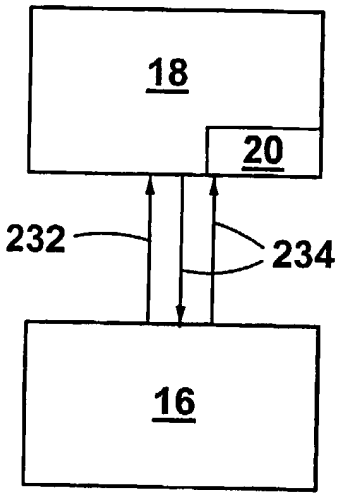


FIG 15



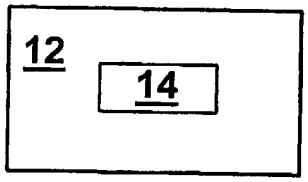


FIG 16

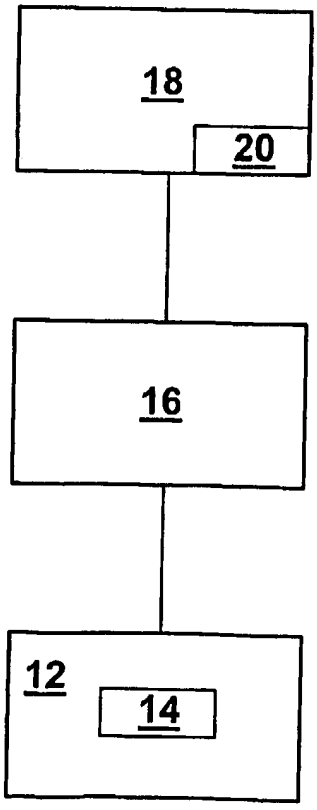


FIG 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 03/02860-0

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: B65D 90/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: B65D, G01S, G08G, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99/12140 A1 (Skygate B.V.) 11 March 1999 (11.03.99) *page 5, lines 12-23.*	1-45
A	US 4750197 A (Mark L. Denekamp) 7 June 1988 (07.06.88) *column 4, lines 6-8,33-43.*	1-15,39-45
A	EP 0748083 A1 (General Electric Company) 11 December 1996 (11.12.96) *fig. 1-5.*	16-38
A	WO 01/98795 A2 (Winko Satellite Limited) 27 December 2001 (27.12.01) *fig. 1.*	16-38

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed

„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 October 2003 (22.10.2003)	20 November 2003 (20.11.2003)
Name and mailing adress of the ISA/AT Austrian Patent Office Dresdner Straße 87, A-1200 Vienna Facsimile No. 1/53424/535	Authorized officer STAWA R. Telephone No. 1/53424/457

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 03/02860-0

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 46-51
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The matter for which protection is sought in claims 46-51 is not characterized in terms of the technical features of invention (Rule 6.3 PCT).

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 03/02860-0

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
EP	A	748083		IL	A	118282	2000-02-17
				US	A	5686888	1997-11-11
				JP	A	9120410	1997-05-06
				EP	A	0748083	1996-12-11
				CA	A	2176879	1996-12-08
US	A	4750197	1988-06-07	US	A	4688244	1987-08-18
WO	A	198795				none	
WO	A	9912140	1999-03-11	JP	T	2001515288T	2001-09-18
				NZ	A	503161	2001-08-31
				CA	A	2302954	1999-03-11
				AU	A	4223297	1999-03-22